

1/5/2 (Item 2 from file: 351) [Links](#)

Fulltext available through: [Order File History](#)

Derwent WPI

(c) 2008 Thomson Reuters. All rights reserved.

0012930583 & *Drawing available*

WPI Acc no: 2003-007169/**200301**

XRPX Acc No: N2003-006167

User identification method involves selecting print data in desired language, corresponding to input ID data of user and analyzing user voice while reading print data

Patent Assignee: SHARP KK (SHAF)

Inventor: AZUMA K

Patent Family (1 patents, 1 & countries)

| Patent Number | Kind | Date | Application Number | Kind | Date | Update | Type |
|---------------|------|----------|--------------------|------|----------|--------|------|
| JP 2002304379 | A | 20021018 | JP 2001107846 | A | 20010405 | 200301 | B |

Priority Applications (no., kind, date): JP 2001107846 A 20010405

Patent Details

| Patent Number | Kind | Lan | Pgs | Draw | Filing Notes |
|---------------|------|-----|-----|------|--------------|
| JP 2002304379 | A | JA | 9 | 7 | |

Alerting Abstract JP A

NOVELTY - A print data in desired language corresponding to input ID of a user, is selected by a server (2). The voice of the user while reading the print data, is analyzed and the analysis result is compared with a value stored in a storage medium, for identifying the user.

DESCRIPTION - An INDEPENDENT CLAIM is included for user identification system.

USE - For identifying user.

ADVANTAGE - Eliminates the need for carrying the credit cards and debit cards and increases the safety.

DESCRIPTION OF DRAWINGS - The figure shows the block diagram of the user identification system. (Drawing includes non-English language text).

2 Server

Title Terms /Index Terms/Additional Words: USER; IDENTIFY; METHOD; SELECT; PRINT; DATA; LANGUAGE; CORRESPOND; INPUT; ID; VOICE; READ

Class Codes

International Patent Classification

| IPC | Class Level | Scope | Position | Status | Version Date |
|--------------|-------------|-------|----------|--------|--------------|
| G06F-0015/00 | A | I | | R | 20060101 |
| G06F-0021/20 | A | I | F | R | 20060101 |
| G10L-0015/00 | A | I | L | R | 20060101 |
| G10L-0015/06 | A | I | L | R | 20060101 |
| G10L-0017/00 | A | I | L | R | 20060101 |
| G06F-0015/00 | C | I | | R | 20060101 |
| G06F-0021/20 | C | I | F | R | 20060101 |
| G10L-0015/00 | C | I | L | R | 20060101 |
| G10L-0017/00 | C | I | L | R | 20060101 |

File Segment: EngPI; EPI;

DWPI Class: T01; T05; W04; P86

Manual Codes (EPI/S-X): T01-C08A; T01-J05B4P; T01-J18; T01-N01A1; T01-N02B1B; T05-L02; W04-V04A3

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2002-304379

(P2002-304379A)

(43) 公開日 平成14年10月18日 (2002. 10. 18)

(51) Int.Cl.⁷

識別記号

F I

テームコード* (参考)

G 0 6 F 15/00

3 3 0

G 0 6 F 15/00

3 3 0 F 5 B 0 8 5

G 1 0 L 15/00

G 1 0 L 3/00

5 4 5 A 5 D 0 1 5

15/06

5 2 1 P

17/00

5 5 1 A

審査請求 未請求 請求項の数 8 O L (全 9 頁)

(21) 出願番号 特願2001-107846(P2001-107846)

(22) 出願日 平成13年4月5日 (2001. 4. 5)

(71) 出願人 000005049

シャープ株式会社

大阪府大阪市阿倍野区長池町22番22号

(72) 発明者 東 賢一

大阪府大阪市阿倍野区長池町22番22号 シ

ャープ株式会社内

(74) 代理人 100078282

弁理士 山本 秀策

Fターム(参考) 5B085 AE02 AE23 AE27

5D015 AA03 AA04 BB01 GG03 GG06

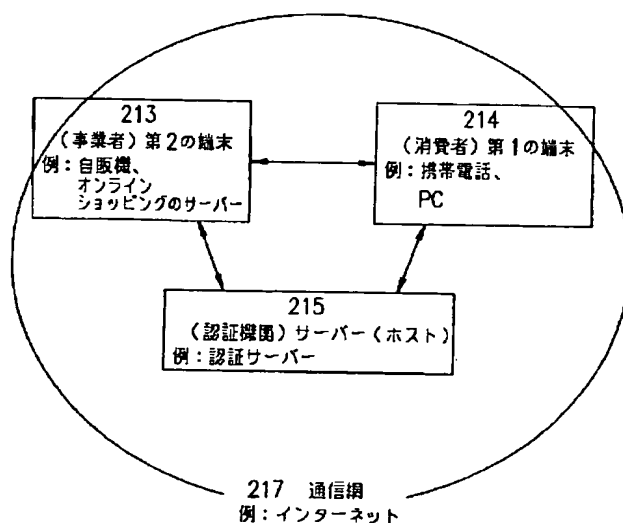
HH04

(54) 【発明の名称】 個人認証方法および個人認証システム

(57) 【要約】

【課題】 肉声に由来する声紋を個人認証のセキュリティの鍵として用いて、安全性を高めた個人認証方法および個人認証システムを提供する。

【解決手段】 被認証者単位で複数の言葉とそれらの言葉を被認証者に発声させたときの声紋データを予め記憶媒体にデータ242として記憶させておき、被認証者から入力されたIDデータに対応する複数の言葉のうちの任意の1つとそれに対応する声紋データを選択する。その言葉を被認証者に提示して発声させ、音声処理解析部244により声紋を解析して記憶媒体から選択した声紋データと照合する。両者が一致した場合にその被認証者を個人認証する。



【特許請求の範囲】

【請求項1】 被認証者から該被認証者のIDデータが認証手段に入力されたときに、

該認証手段は、被認証者単位で複数の言葉とそれらの言葉を被認証者に発声させたときの声紋データを予め記憶させておいた記憶媒体から、入力されたIDデータに対応する複数の言葉のうちの任意の1つとそれに対応する声紋データを選択して、

選択された言葉を被認証者に提示し、提示した言葉を被認証者に発声させて声紋を解析し、

解析結果と該記憶媒体から選択された声紋データとを照合して、両者が一致した場合にその被認証者を個人認証することを特徴とする個人認証方法。

【請求項2】 被認証者から該被認証者のIDデータが認証手段に入力されたときに、

該認証手段は、押複数の言葉を含む一覧データ表と被認証者の基本単位の声紋データを予め記憶させておいた記憶媒体から、該一覧データ表に含まれた複数の言葉のうちの任意の1つを選択すると共に、入力されたIDデータに対応する基本単位の声紋データを選択された言葉の配列に配列して声紋データを生成して、選択された言葉を被認証者に提示し、提示した言葉を被認証者に発声させて声紋を解析し、

解析結果と基本単位の声紋データから生成された声紋データとを照合して、両者が一致した場合にその被認証者を個人認証することを特徴とする個人認証方法。

【請求項3】 前記記憶媒体から複数の言葉のうちの任意の1つを選択する際に、前記認証手段の内部に格納されている乱数発生プログラムを用いる請求項1または請求項2に記載の個人認証方法。

【請求項4】 前記認証手段は、前記記憶媒体から複数の言葉のうちの任意の2つ以上を選択する請求項1乃至請求項3のいずれかに記載の個人認証方法。

【請求項5】 被認証者が操作する第1の操作手段と、該被認証者の認証を要求する第2の操作手段と、該被認証者の認証を行う認証手段とが通信網を介して接続されているシステムにおいて、

該認証手段は、少なくとも、被認証者単位で複数の言葉とそれらの言葉を被認証者に発声させたときの声紋データを予め記憶しておく記憶媒体と、

被認証者が第1の操作手段から入力した該被認証者のIDデータが通信網を介して該認証手段に伝えられたときに、該記憶媒体から、該IDデータに対応する複数の言葉のうちの任意の1つとそれに対応する声紋データを選択して選択された言葉を該通信網を介して被認証者に提示する手段と、

提示した言葉を被認証者が発声した声を通信網を介して入力して声紋を解析する解析手段と、

解析結果と該記憶媒体から選択された声紋データとを照合する照合手段とを有することを特徴とする個人認証シ

ステム。

【請求項6】 被認証者が操作する第1の操作手段と、該被認証者の認証を要求する第2の操作手段と、該被認証者の認証を行う認証手段とが通信網を介して接続されているシステムにおいて、

該認証手段は、少なくとも、複数の言葉を含む一覧データ表と被認証者の基本単位の声紋データを予め記憶させておく記憶媒体と、

被認証者が第1の操作手段から入力した該被認証者のIDデータが通信網を介して該認証手段に伝えられたときに、該記憶媒体から、該一覧データ表に含まれた複数の言葉のうちの任意の1つを選択すると共に、入力されたIDデータに対応する基本単位の声紋データを選択された言葉の配列に配列して声紋データを生成して、選択された言葉を該通信網を介して被認証者に提示する手段と、

提示した言葉を被認証者が発声した声を通信網を介して入力して声紋を解析する解析手段と、

解析結果と基本単位の声紋データから生成された声紋データとを照合する照合手段とを有することを特徴とする個人認証システム。

【請求項7】 前記認証手段は、前記記憶媒体から複数の言葉のうちの任意の1つを選択する際に使用する乱数発生プログラムが内部に格納されている請求項5または請求項6に記載の個人認証システム。

【請求項8】 前記認証手段は、前記記憶媒体から複数の言葉のうちの任意の2つ以上を選択する請求項5乃至請求項7のいずれかに記載の個人認証システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、安全性を有する個人認証方法および個人認証システムに関し、特に、消費者側操作端末と事業者側操作端末と認証サーバー等のホストコンピューターとがインターネット等の通信網を介して接続されているシステムに好適な個人認証方法および個人認証システムに関する。

【0002】

【従来の技術】従来、操作端末からホストコンピューターへのアクセス許可を得る方法として、暗証番号やパスワードを操作端末から入力して、ホストコンピューターが有するそれらのデータと照合することにより個人認証を行ってホストコンピューターへのアクセス許可を与えるものが知られている。

【0003】しかし、近年、インターネット等のネットワークを利用した電子商取引が活発化するにつれて、より安全性の高い個人認証方法（セキュリティ）が求められている。

【0004】このようなより安全性の高い個人認証方法として、例えば特開平10-21305号公報に記載されている認証方法が挙げられる。この公報の技術は、各

30

40

50

人固有の特徴である声紋、角膜紋、指紋、指の骨格および顔面パターンを個人認証（セキュリティ）の鍵として利用する電子商取引システムを構築し、商品購入者と商店との間に第3者機関としての認証サーバーを設けて、これをインターネット等の公共通信網により結び付けているものである。

【0005】この従来技術は、図7に示すように、インターネット10に接続され、商品購入希望者が購入したい商品の情報を受信する商店の端末装置11と、商品購入希望者から、その商品購入希望者固有の身体的特徴の情報とこれを検索するための検索コードとを商品購入希望についての情報に付加して認証サーバー（ホストコンピュータ）13に送信する情報処理装置12と、認証を行う認証サーバー13からシステムが構成される。

【0006】認証サーバー13は、商品購入希望者固有の身体的特徴の情報を、被照合情報として検索コードに対応させて記憶しているメモリ13eを有し、情報処理装置12から送信された商品購入希望者の身体的特徴の情報と検索コードと商品購入希望についての情報とを受信して、受信した身体的特徴の情報と、検索コードにより検索した身体的特徴の情報とが一致しているか否かを判定する。そして、それらが一致しているときに本人であるという認証を行い、商店の端末装置11に商品購入希望についての情報を送信する。ここでは、購入者固有の身体的特徴として、声紋、角膜紋、指紋、指の骨格および顔面パターンが例示されている。

【0007】なお、この図7において、14は情報処理装置12のMPUであり、15は電子取引処理プログラム15a、認証通信処理プログラム15b、暗号化処理プログラム15cおよび認証データ生成プログラム15d等を格納したメモリであり、16はメモリ16aを有する音声入力装置であり、17はマイクロホンである。また、13aは認証サーバー13において送信されたデータを復元する解読回路であり、13bは特徴抽出処理回路であり、13cはMPUであり、13はIDパターン記憶部131、標準IDパターンテーブル132、DPマッチング処理プログラム133、データ送信プログラム134等を有するメモリである。

【0008】

【発明が解決しようとする課題】上述した特開平10-21305号公報の従来技術において、利用される個人認証（セキュリティ）の鍵のうち、角膜紋、指紋、指の骨格および顔面パターンについては、これらのデータが認証サーバー13内のメモリに格納されている。これらの格納データ、または情報処理装置12から取り込んで認証サーバー13に転送中のデータを、一旦何らかの手法により第三者に盗み取られた場合、その身体的特徴は個人固有のものであるが故に、セキュリティの鍵を変更することはほとんど不可能である。

【0009】また、上記従来技術においては、上記デー

タの暗号化によるセキュリティ向上についても考慮されている。しかし、その暗号が解読された場合には、やはり各人固有の身体的特徴であるが故に、セキュリティの鍵を変更することは困難である。

【0010】さらに、上記従来技術において、もう1つのセキュリティの鍵である声紋については、商品購入希望者が認証を受けるときに自らが選んだ暗証コードと音声IDデータ（肉声または肉声に由来する声紋）を使用する。しかし、この方法では、悪意を有する者に暗証コードを盗み取られ、さらに音声IDデータを録音されてしまうおそれがある。例えば、操作端末からの入力がある公共の場所、例えばデパートメントストアにおいてショッピングを行っている場合や自動販売機からの商品購入時における利用を考えると、その公共性の故に上記問題が重要になる。

【0011】従って、上記従来技術は、安全性の高い個人認証システムであるとは言えない。

【0012】本発明は、肉声に由来する声紋を個人認証のセキュリティの鍵として用い、さらに安全性を高めた個人認証方法および個人認証システムを提供することを目的とする。

【0013】

【課題を解決するための手段】本発明の個人認証方法は、被認証者から該被認証者のIDデータが認証手段に入力されたときに、該認証手段は、被認証者単位で複数の言葉とそれらの言葉を被認証者に発声させたときの声紋データを予め記憶させておいた記憶媒体から、入力されたIDデータに対応する複数の言葉のうちの任意の1つとそれに対応する声紋データを選択して、選択された言葉を被認証者に提示し、提示した言葉を被認証者に発声させて声紋を解析し、解析結果と該記憶媒体から選択された声紋データとを照合して、両者が一致した場合にその被認証者を個人認証することを特徴とする。

【0014】上記方法によれば、消費者を認証するための鍵となる「言葉」を、例えば日時等により認証手段側で任意に変えることができ、デパートメントストアや商店、自動販売機、銀行のATM等の公共の場所であっても、悪意を有する者が存在するおそれがある場所においても、高いセキュリティを維持することが可能である。

【0015】本発明の個人認証方法は、被認証者から該被認証者のIDデータが認証手段に入力されたときに、該認証手段は、複数の言葉を含む一覧データ表と被認証者の基本単位の声紋データを予め記憶させておいた記憶媒体から、該一覧データ表に含まれた複数の言葉のうちの任意の1つを選択すると共に、入力されたIDデータに対応する基本単位の声紋データを選択された言葉の配列に配列して声紋データを生成して、選択された言葉を被認証者に提示し、提示した言葉を被認証者に発声させて声紋を解析し、解析結果と基本単位の声紋データから生成された声紋データとを照合して、両者が一致した場

合にその被認証者を個人認証することの特徴とする。

【0016】上記方法によれば、基本単位の声紋データを選択された言葉の配列に配列して声紋データを作成するため、声紋データを記憶しておくメモリ容量が少なく済み、消費者を認証するための鍵となる「言葉」の選択が増える。また、消費者は基本単位の言葉を発声して登録するだけでよく、「言葉」は認証の都度、変えられることから、さらに高いセキュリティを維持することが可能である。

【0017】前記記憶媒体から複数の言葉のうちの任意の1つを選択する際に、前記認証手段の内部に格納されている乱数発生プログラムを用いてもよい。

【0018】上記方法によれば、セキュリティの鍵となる「言葉」を無秩序に選択することができるので、高いセキュリティを維持することが可能である。

【0019】前記認証手段は、前記記憶媒体から複数の言葉のうちの任意の2つ以上を選択してもよい。

【0020】本発明の個人認証システムは、被認証者が操作する第1の操作手段と、該被認証者の認証を要求する第2の操作手段と、該被認証者の認証を行う認証手段とが通信網を介して接続されているシステムにおいて、該認証手段は、少なくとも、被認証者単位で複数の言葉とそれらの言葉を被認証者に発声させたときの声紋データを予め記憶させておく記憶媒体と、被認証者が第1の操作手段から入力した該被認証者のIDデータが通信網を介して該認証手段に伝えられたときに、該記憶媒体から、該IDデータに対応する複数の言葉のうちの任意の1つとそれに対応する声紋データを選択して選択された言葉を該通信網を介して被認証者に提示する手段と、提示した言葉を被認証者が発声した声を通信網を介して入力して声紋を解析する解析手段と、解析結果と該記憶媒体から選択された声紋データとを照合する照合手段とを有することを特徴とする。

【0021】上記構成によれば、消費者を認証するための鍵となる「言葉」を、例えば日時等により認証手段側で任意に変えることができ、デパートメントストアや商店、自動販売機、銀行のATM等の公共の場所であっても、悪意を有する者が存在するおそれがある場所においても、高いセキュリティを維持することが可能である。

【0022】本発明の個人認証システムは、被認証者が操作する第1の操作手段と、該被認証者の認証を要求する第2の操作手段と、該被認証者の認証を行う認証手段とが通信網を介して接続されているシステムにおいて、該認証手段は、少なくとも、複数の言葉を含む一覧データ表と被認証者の基本単位の声紋データを予め記憶させておく記憶媒体と、被認証者が第1の操作手段から入力した該被認証者のIDデータが通信網を介して該認証手段に伝えられたときに、該記憶媒体から、該一覧データ表に含まれた複数の言葉のうちの任意の1つを選択すると共に、入力されたIDデータに対応する基本単位の声

紋データを選択された言葉の配列に配列して声紋データを生成して、選択された言葉を該通信網を介して被認証者に提示する手段と、提示した言葉を被認証者が発声した声を通信網を介して入力して声紋を解析する解析手段と、解析結果と基本単位の声紋データから生成された声紋データとを照合する照合手段とを有することを特徴とする。

【0023】上記構成によれば、基本単位の声紋データを選択された言葉の配列に配列して声紋データを作成するため、声紋データを記憶しておくメモリ容量が少なく済み、消費者を認証するための鍵となる「言葉」の選択が増える。また、消費者は基本単位の言葉を発声して登録するだけでよく、「言葉」は認証の都度、変えられることから、さらに高いセキュリティを維持することが可能である。

【0024】前記認証手段は、前記記憶媒体から複数の言葉のうちの任意の1つを選択する際に使用する乱数発生プログラムが内部に格納されていてもよい。

【0025】上記構成によれば、セキュリティの鍵となる「言葉」を無秩序に選択することができるので、高いセキュリティを維持することが可能である。

【0026】前記認証手段は、前記記憶媒体から複数の言葉のうちの任意の2つ以上を選択してもよい。

【0027】

【発明の実施の形態】以下に、本発明の実施の形態について、図面を参照しながら説明する。

【0028】（実施形態1）図1は、本発明の一実施形態である個人認証システムの構成を示すブロック図である。ここでは、個人認証に関する部分のみを示しており、少なくとも消費者が操作を行う第1の操作端末214、事業者が操作を行う第2の操作端末213、認証機関が操作を行うサーバー（ホストコンピューター）、およびこれらを結ぶインターネット等の通信網217から構成されている。

【0029】第1の操作端末214は、消費者側に設けられるものである。例えば、携帯電話に代表される移动通信端末やパーソナルコンピュータの端末等が挙げられる。

【0030】この第1の操作端末214は、図2に示すように、少なくともMPU231と、消費者が発声する音声を入力するためのマイクロホン233と、マイクロホン233から取り込んだ音声をデジタル信号に変換するA/D変換手段を含む音声処理部232と、デジタル化した音声デジタルを一旦記憶させるメモリ232aと、電子商取引プログラムを格納した領域234a、認証処理を行うための認証サーバー（ホストコンピューター）215とやり取りを行うための認証通信処理プログラムを格納した領域234bを含むメモリ領域234から構成され、これらがバスライン230により接続されている。なお、メモリ領域234cおよび234dにつ

いては後述するが、本実施形態では省略可能である。

【0031】また、第2の操作端末213は、例えば自動販売機やオンラインショッピングを行う商店（インターネット上の仮想商店も含む）、チケットや宿泊等の予約を行うための操作端末等が挙げられる。

【0032】この第2の操作端末213は、図3に示すように、少なくともMPU221と、例えば商品の品番、仕様、その販売価格や商品画像等の商品情報一覧を格納したデータメモリ領域222と、電子商品取引プログラムを格納した領域223aを含むメモリ領域223から構成され、これらがバスライン220により接続されている。

【0033】なお、上記第1の操作端末214の機能と第2の操作端末213の機能が融合されて1つの操作端末を構成していてもよい。例えば自動販売機やオンラインショッピングを行う商店（インターネット上の仮想商店も含む）、チケットや宿泊等の予約を行うための操作端末、銀行のキャッシュディスペンサ等が挙げられる。

【0034】さらに、認証機関のサーバー（ホストコンピュータ）215は、図4に示すように、少なくともMPU241と、複数の言葉とその言葉の肉声に由来する声紋からなる組み合わせデータが格納されているデータメモリ領域242と、第1の操作端末214から受信したデジタル化された音声データから声紋を抽出し、データメモリ領域242に格納されているデータと照合解析する音声処理部244と、電子商取引プログラムを格納した領域243a、第1の操作端末214や第2の操作端末213とやり取りを行うための認証通信処理プログラムを格納した領域243b、上記音声処理部を行って認証を行うための認証可否処理プログラムを格納した領域243cを含むメモリ領域243から構成され、これらがバスライン240により接続されている。なお、メモリ領域243cおよび243dについては後述するが、本実施形態では省略可能である。

【0035】以下に、本実施形態の個人認証システムにおける、商品購入や予約等を希望する消費者の個人認証を含む処理手順について、図5のフローチャートを参照しながら説明する。まず、ステップ201において、消費者は第1の操作端末214を操作し、インターネット等の通信網217を経由して事業者（商店等）に備えられた第2の操作端末213に働きかけて、データメモリ領域222に格納されている商品の品番、仕様、その販売価格や商品画像等の商品情報一覧を参照して、所望の商品と数量（以後、商品情報と称する）を選択する。

【0036】次に、ステップ202において、第2の操作端末213は、確認のために第1の操作端末214に受信した消費者からの商品情報にその購入金額を加えた情報を第1の操作端末214に返送する。

【0037】続いて、ステップ203において、消費者は第1の操作端末214により、第2の操作端末213

から送信されてきた商品情報とその購入金額を確認する。そして、消費者はその内容に問題がある場合には不承認としてステップ201に戻し、一方、内容に問題が無い場合には承認して次のステップ204に進む。

【0038】ステップ204では、消費者は承認した商品情報とその購入金額と共に、消費者を識別するID番号（暗証番号やパスワード等、但し、第1の操作端末214が携帯電話等であって、予め電話番号等、IDに相当するものが登録されている場合には、暗証番号やパスワードをさらに入力することを省略することができる。）を第1の操作端末214から認証機関側に備えられたサーバー215に送信する。なお、ID番号（数字）の代りにアルファベット等の英数字を用いてもよい。

【0039】その後、ステップ205において、サーバー215は、内蔵している記憶媒体（データメモリ領域242）から消費者固有のID番号を検索する。そして、サーバー215は、消費者から入力されたID番号が記憶媒体に記憶されていない場合には以降の処理を拒否してステップ204に戻し、一方、ID番号が記憶媒体に記憶されている場合にはステップ206に進む。

【0040】ステップ206では、サーバー215は、データメモリ領域242から、消費者固有のID番号に対応したセキュリティの鍵として活用する複数の暗証コード（例えば「山」、川等の言葉と、その言葉を消費者が発声した際の声紋データとの組み合わせ）の中から1組の暗証コードを選択する。これらの複数の暗証コードは、ID番号と共に、予めデータメモリ領域242に登録しておく。このときの暗証コード（言葉）の選択の仕方は、悪意を有する者にとって予測困難であるように選択するのが好ましい。例えば、サーバー内にタイマー機能を設けることにより、複数の暗証コードの中から選択される暗証コードを変えることができる。さらにセキュリティを向上させるためには、例えば、サーバー215内に乱数発生プログラム等を内蔵させ（例えばメモリ243に格納し）、これを利用して複数の暗証コードの中から1つの暗証コードを選択することができる。

【0041】次に、ステップ207において、サーバー215は、データメモリ領域242から選択した1組の暗証コード（「言葉」とその言葉を消費者が発声した際の声紋データ）を、消費者側に備えられた第1の操作端末214へ送信する。

【0042】送信された「言葉」は、例えば第1の操作端末214の画面（図示せず）に表示される。続いて、ステップ208において、消費者は画面に表示された「言葉」を第1の操作端末214のマイクロホン233に向かって発声する。第1の操作端末214の音声処理部232は、入力された「言葉」をA/D変換してデジタル化し、そのデジタル音声データをサーバー215に送信する。その後、ステップ209において、サーバー

215は受信した消費者が発声したデジタル音声データを音声処理解析部244により声紋データに変換し、この声紋データと先のステップ206で選択されたデータメモリ領域242内の声紋データとを比較する。そして、サーバー215は声紋データが不一致である場合はステップ208に戻し、一方、一致している場合には本人であると認証して、事業者側に備えられた第2の操作端末(第2の操作端末が含まれているものであってもよい)213にその結果を送信する。

【0043】これにより、図示はしていないが、次のステップとして、事業者は消費者への商品の発送手続きまたはチケット発売や予約手続き、或いは銀行のキャッシュディスペンサであれば引出処理等を行うと共に、それに要した代金をプリペイドカード(インターネット上の仮想プリペイドカードも含む)からの引き落とししたり、またはサーバー215を通じて金融機関に代金を通知して消費者の講座からの引き落としや振り込み処理を行って、事前または事後に、消費者から商品の購入代金を事業者の口座等に払い込ませる。

【0044】さらに、セキュリティを強化するためには、ステップ208において、消費者が発声した「言葉」をデジタル変換した後、第1の操作端末214のメモリ234に格納された暗号化処理プログラム234cを活用して暗号化して、サーバー215に送信する手法も有効である。この場合、サーバー215は受信した音声デジタルをメモリ243に格納された復号化処理プログラム243dを活用して復号してから声紋データに変換する。そして、サーバー215は、データメモリ領域242に記憶された複数の暗証データの中から1組の暗証コード(「言葉」とその声紋データ)を選択し、その選択された暗証コードの「言葉」をメモリ領域242eに格納されている暗号化処理プログラムを活用して暗号化して、消費者側に備えられた第1の操作端末214へ送信する。第1の操作端末214は、メモリ領域234dに格納されている復号化処理プログラムを活用して「言葉」に復号し、画面に表示することができる。

【0045】なお、本実施形態では1組の暗証コードを選択した例について説明したが、セキュリティを高めるためには、複数の暗証コードを選択して組み合わせてもよい。例えば、複数の暗証コードを選択して組み合わせる場合には、複数の暗証コードの「言葉」を消費者側の第1の操作端末214に送信して消費者に複数の言葉を発声させるようにする。さらに、認証不一致により再度認証を試みる場合に、選択される「言葉」を変えるようにしてもよい。

【0046】(実施形態2)以下に、本実施形態の個人認証システムにおける、商品購入や予約等を希望する消費者の個人認証を含む処理手順について、図6のフローチャートを参照しながら説明する。本実施形態では、上記実施形態1と異なり、サーバー215の記憶媒体(デ

ータメモリ領域242)に消費者が発声した言葉(意味のある言葉としての声紋データ)を記憶しておかず、認証機関が用意した言葉、例えば「山」、「川」、・・・等の言葉の一覧データ表と、消費者が発声した基本単位(50音)の声紋データ、例えば「あ、い、う、え、お、・・・」等の声紋データのみを記憶しておく。

【0047】ステップ301～ステップ305までは、上記実施形態1のステップ201～ステップ205と同様であるので、ここでは説明を省略する。

10 【0048】ステップ306では、消費者が入力したID番号がサーバー内の記憶媒体(データメモリ領域242)に記憶されていることを確認したサーバー215は、データメモリ領域242から、認証機関が用意した言葉の一覧データ表からランダムに1つの言葉を選択する。これは、上記実施形態1とは異なり、消費者のID番号に依存した暗証コードではない。このときの言葉の選択の仕方は、悪意を有する者にとって予測困難であるように選択するのが好ましく、例えば、サーバー215内に乱数発生プログラム等を内蔵させ、これを利用して言葉の一覧データ表から1つの言葉を選択することがで

20 【0049】次に、ステップ307では、消費者固有のID番号に対応してデータメモリ領域242に記憶されている基本の声紋データを、選択された「言葉」に対応した声紋の配列に配列して、声紋データを生成する。

【0050】続いて、ステップ308において、サーバー215は、データメモリ領域242から選択した「言葉」を、消費者側に備えられた第1の操作端末214へ送信する。

30 【0051】送信された「言葉」は、例えば第1の操作端末214の画面(図示せず)に表示され、または音声出力される。続いて、ステップ309において、消費者は画面に表示され、または音声出力された「言葉」を第1の操作端末214のマイクロホン233に向かって発声する。第1の操作端末214の音声処理部232は、入力された「言葉」をA/D変換してデジタル化し、音声処理部内のメモリ領域232aに一旦記憶した後、暗号化処理等を行い、そのデジタル音声データをサーバー215に送信する。

40 【0052】その後、ステップ310において、サーバー215は受信した消費者が発声したデジタル音声データを音声処理解析部244により声紋データに変換し、この声紋データと先のステップ307で生成された声紋データとを比較する。

【0053】その後の認証可否と、本人認証後の処理は上記実施形態1と同様であるので、ここでは説明を省略する。

50 【0054】さらに、セキュリティを強化するためには、ステップ309において、消費者が発声した「言葉」をデジタル変換した後、第1の操作端末214のメ

メモリ 234 に格納された暗号化処理プログラム 234c を活用して暗号化して、サーバー 215 に送信する手法も有効である。この場合、サーバー 215 は受信した音声デジタルをメモリ 243 に格納された復号化処理プログラム 243d を活用して復号してから声紋データに変換する。そして、サーバー 215 は、データメモリ領域 242 に記憶された言葉の一覧データ表から 1 つの「言葉」を選択し、その選択された「言葉」をメモリ領域 242e に格納されている暗号化処理プログラムを活用して暗号化して、消費者側に備えられた第 1 の操作端末 214 へ送信する。第 1 の操作端末 214 は、メモリ領域 234d に格納されている復号化処理プログラムを活用して「言葉」に復号し、画面に表示し、またはスピーカ（図示せず）から音声出力することができる。

【0055】なお、本実施形態では 1 つの言葉を選択した例について説明したが、セキュリティを高めるためには、複数の「言葉」を選択して組み合わせてもよい。さらに、認証不一致により再度認証を試みる場合に、選択される「言葉」を変えるようにしてもよい。

【0056】

【発明の効果】以上詳述したように、本発明によれば、消費者を認証するための鍵となる「言葉」を、例えば日時等により認証手段側で任意に変えることができるので、デパートメントストアや商店、自動販売機、銀行の ATM 等の公共の場所であって、悪意を有する者が存在するおそれがある場所においても、高いセキュリティを維持することができる。

【0057】さらに、他の本発明によれば、被認証者の基本単位の声紋データのみを認証手段（サーバー）内に記憶させ、選択された言葉の配列に配列して声紋データを作成するため、声紋データを記憶しておくメモリ容量が少なく済み、消費者を認証するための鍵となる「言葉」の組み合わせを増やすことができるため、選択可能な「言葉」を増やすことができる。また、消費者は基本単位の言葉を発声して登録するだけでよく、「言葉」は認証の都度、変えられることから、さらに高いセキュリティを維持することができる。

【0058】従って、消費者はクレジットカードやデビットカード等を携帯する必要がなくなる。

【図面の簡単な説明】

【図 1】本発明の一実施形態である個人認証システムの構成を説明するためのブロック図である。

【図 2】本発明の実施形態に係る第 1 の操作端末の構成を説明するためのブロック図である。

【図 3】本発明の実施形態に係る第 2 の操作端末の構成を説明するためのブロック図である。

【図 4】本発明の実施形態に係る認証手段（サーバー）の構成を説明するためのブロック図である。

【図 5】実施形態 1 の個人認証方法について説明するためのフローチャートである。

【図 6】実施形態 2 の個人認証方法について説明するためのフローチャートである。

【図 7】従来の個人認証システムの構成を説明するためのブロック図である。

【符号の説明】

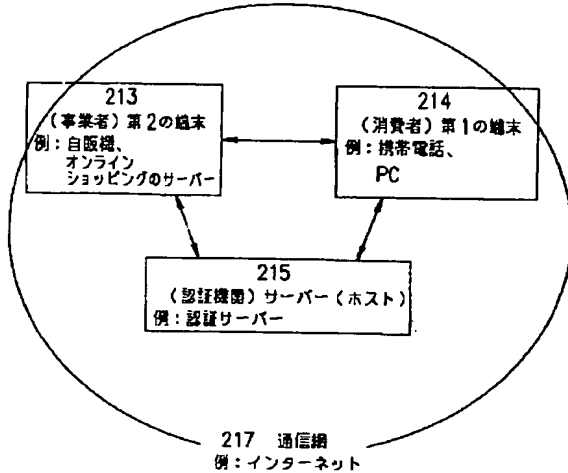
- 10 インターネット
- 11 商店の端末装置
- 12 パーソナルコンピュータ
- 13 認証サーバー
- 13a 解読回路
- 13b 特徴抽出処理回路
- 13c MPU
- 13e メモリ
- 14 MPU
- 15 メモリ
- 15a 電子商取引プログラム
- 15b 認証通信処理プログラム
- 15c 暗号化処理プログラム
- 15d 認証データ生成プログラム
- 20 16 音声入力装置
- 16a メモリ
- 131 ID パターン記憶部
- 132 標準 ID パターンテーブル
- 133 DP マッチング処理プログラム
- 134 データ送信プログラム
- 213 第 2 の端末装置
- 214 第 1 の端末装置
- 215 認証機関（サーバー）
- 217 通信網
- 30 220 バスライン
- 221 MPU
- 222 データ（データメモリ領域）
- 223 メモリ
- 223a 電子商取引プログラム（格納領域）
- 230 バスライン
- 231 MPU
- 232 音声処理部
- 232a メモリ
- 233 マイクロホン
- 40 234 メモリ
- 234a 電子商取引プログラム（格納領域）
- 234b 認証通信処理プログラム（格納領域）
- 234c 暗号化処理プログラム（格納領域）
- 234d 復号化処理プログラム（格納領域）
- 240 バスライン
- 241 MPU
- 242 データ（データメモリ領域）
- 243 メモリ
- 243a 電子商取引プログラム（格納領域）
- 50 243b 認証通信処理プログラム（格納領域）

13

243c 認証可否処理プログラム

243e 暗号化処理プログラム (格納領域)

【図 1】

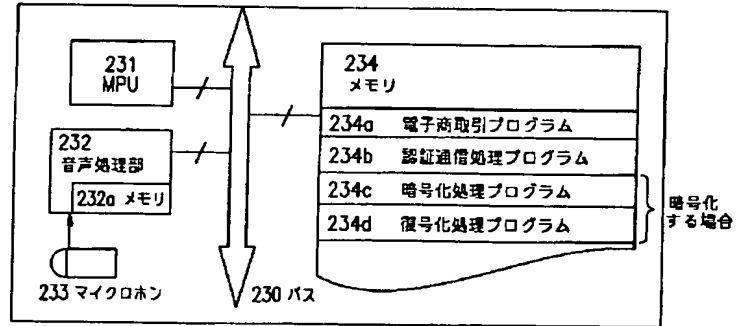


14

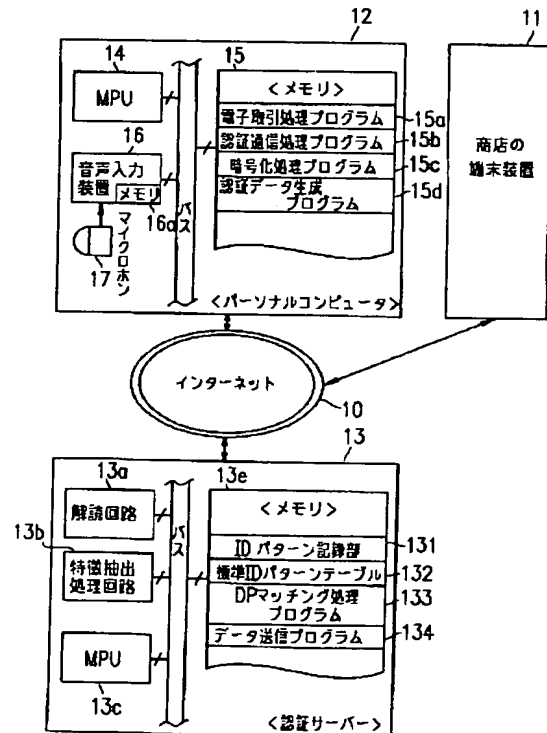
243d 復号化処理プログラム (格納領域)

244 音声処理解析部

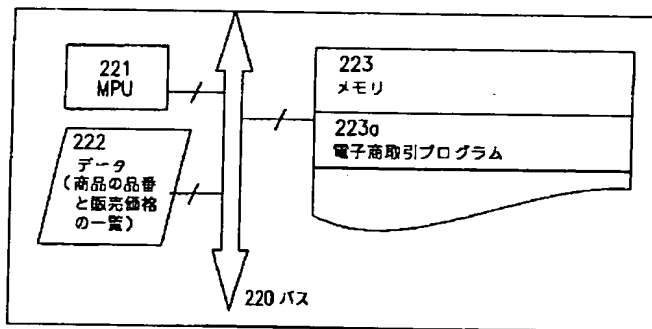
【図 2】



【図 7】



【図 3】



【図 4】

